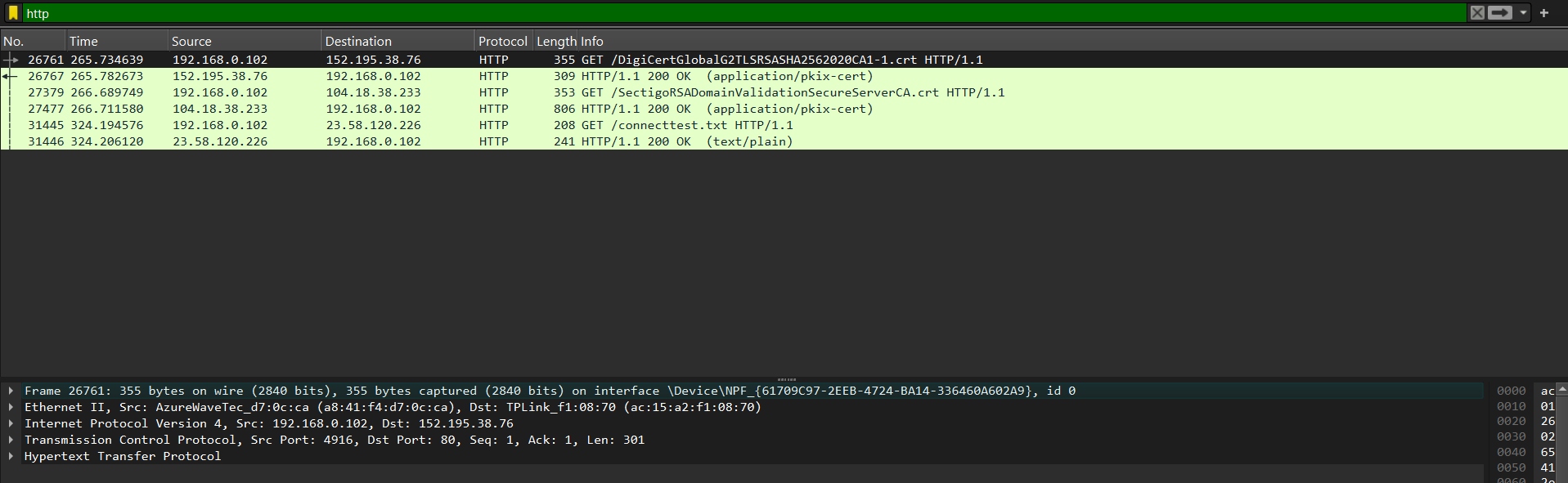
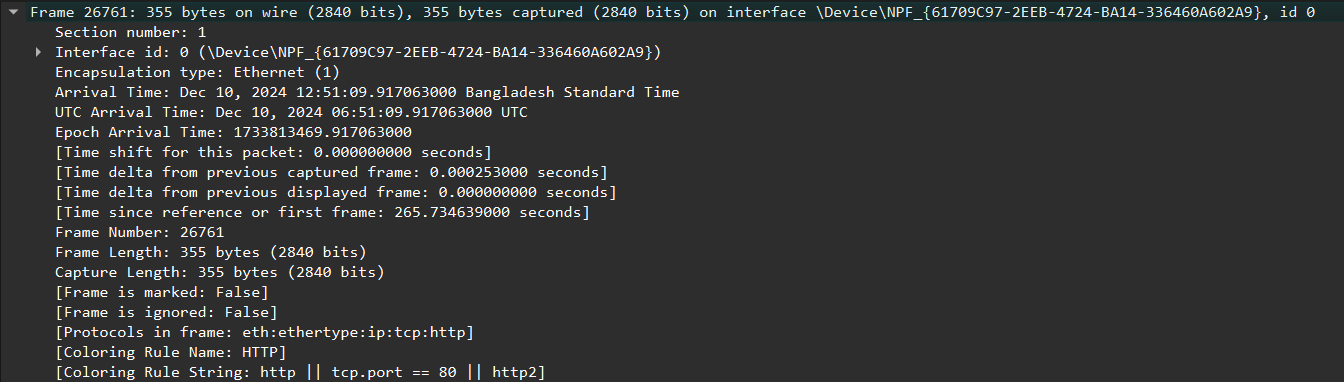
The website that I visited: [**https://www.dghs.gov.bd/**](https://www.dghs.gov.bd/*)

Frame:



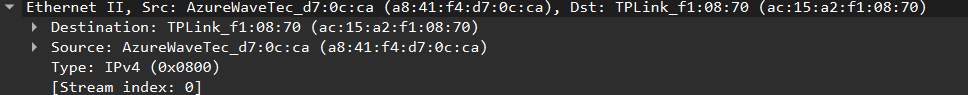
The frame itself is not a standalone layer in the OSI model but is primarily associated with the Data Link Layer (Layer 2) for encapsulation and with the Physical Layer (Layer 1) for transmission.

Ethernet (1) - Indicates that the packet uses Ethernet encapsulation at the data link layer.

Frame Length: 355 bytes (2840 bits) - the actual size of the captured packet.

The Ethernet layer is responsible for transferring frames across the local network using MAC addresses.

Ethernet:



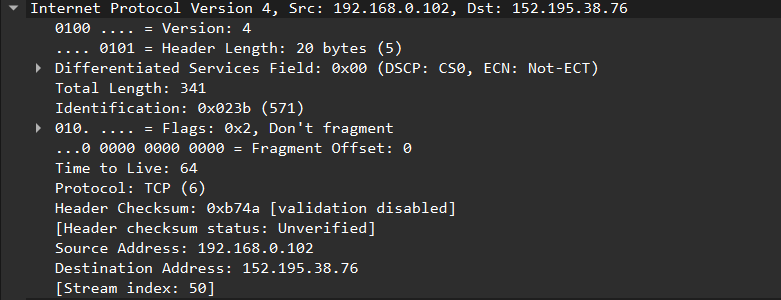
Ethernet II header, which is part of the Data Link Layer.

Source MAC Address: AzureWaveTec\_d7:0c:ca (a8:41:f4:d7:0c:ca) This uniquely identifies the sender on the local network.

Destination MAC Address: TPLink\_f1:08:70 (ac:15:a2:f1:08:70) This identifies the destination within the local network.

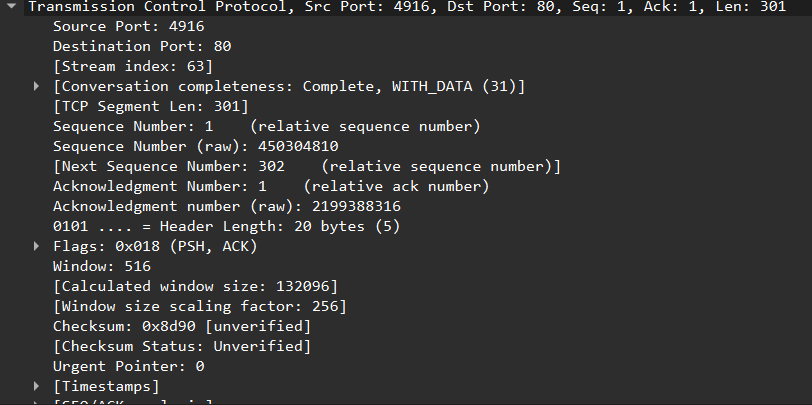
It ensures the packet reaches the correct recipient by using MAC addresses and specifies the encapsulated protocol (in this case, IPv4) for further processing by higher layers.

IPv4:



IPv4 header falls under the Network Layer. It is responsible for routing the packet across networks. It identifies the source and destination IP addresses, handles fragmentation, ensures packet validity (checksum), and prevents loops with the TTL field.

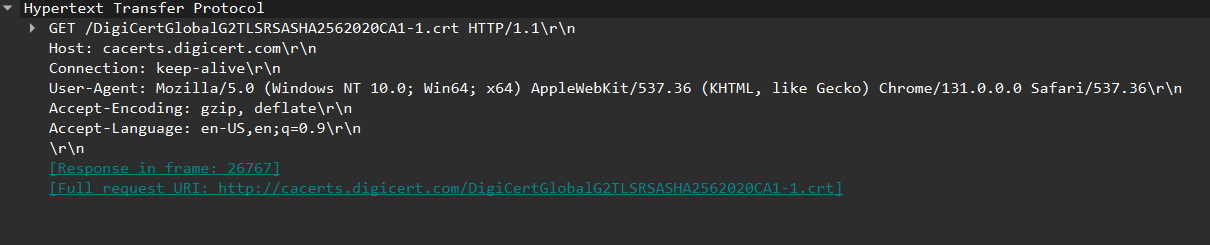
TCP



The client (source port 4916) is sending data to the server on port 80 (HTTP). The packet contains 301 bytes of data and is acknowledging previously received data from the server (ACK flag). The PSH flag indicates the client wants the data to be processed immediately.

The client is allowing the server to send up to 132096 bytes of data before requiring further acknowledgment. The client is sending a chunk of data (possibly part of an HTTP request) to the server and is ready to receive more data from the server up to the advertised window size.

HTTP:



The client (likely a browser or automated tool) is requesting a file (a certificate file) from DigiCert's certificate repository. It uses HTTP/1.1, requests to keep the connection open for efficiency, and specifies that it can handle compressed responses in English.

This is part of a typical process, possibly to verify a secure connection or download an intermediate certificate. The server's response to this request will be in frame 26767.